DMA
Direct Marketing Association

January 19, 2007

Via Electronic Filing (taskforcecomments@idtheft.gov)

The Honorable Alberto R. Gonzalez
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

The Honorable Deborah P. Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Comments to Federal Identity Theft Task Force

Dear Attorney General Gonzalez and Chairman Majoras:

The Direct Marketing Association ("DMA") appreciates the opportunity to comment, in response to the Identity Theft Task Force's ("Task Force") invitation, on several issues regarding recommendations it will make in its final strategic plan to the President.

DMA and its members have for many years been leading custodians of personal information. We have worked hard to provide data security standards and best practices for our members, and to provide educational tools in this area to our valued customers. To this end, we have worked with the Federal Trade Commission ("Commission") on several projects to help businesses and consumers more effectively safeguard personal information.

Several years ago, we worked in cooperation with the Commission to create and disseminate a checklist of security procedures for businesses that collect, store, and transfer personally identifiable information. In 2005, we again partnered with the Commission to print and distribute its *OnGuard Online* brochure, tips for consumers on safer computing. And just last fall, we again partnered with the Commission in its *AvoID Theft* campaign. For this effort, we adapted the Commission's consumer education materials so that our member companies—which have at their disposal millions of daily touchpoints with consumers—can get this relevant and important message to people who need to hear it.

DMA is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. DMA advocates industry standards for responsible marketing; promotes relevance as the key to reaching consumers with desirable offers; and provides cutting-edge research, education, and networking opportunities for marketers. Founded in 1917, DMA today represents more than 3,600 companies from dozens of vertical industries in the U.S. and 50 other nations, including a majority of the *Fortune 100* companies, as well as more than 200 nonprofit organizations.

1. A National Breach Notification Requirement Should be Adopted

The Task Force asks whether "... a breach notification requirement [would] be helpful in addressing any deficiencies in the protocols currently followed by businesses after they suffer a breach." (RFC p. 4) DMA strongly supports the regulation of data security and notification of breaches under a uniform national standard. To date, 34 state laws, some with differing standards, have been enacted, with additional laws likely.

Uniformity both would provide businesses with a standard means of providing notification and create understandable expectations on the part of individuals whose personal information may be the subject of a breach. Uniformity of security requirements would provide similar certainty to businesses to ensure compliance, and would result in effective and enforceable security standards that would benefit individuals.

2. Breach Notification Requirements Should Be Tailored to Apply to Information That is Truly Sensitive

The task force should recommend that breach notification requirements should apply to certain types of sensitive information, the compromise of which could result in identity theft: financial account numbers, social security numbers, and driver's license numbers or their equivalent. In addition, notification should not be required for these data types where they are either truncated, encrypted or protected by similar technological measures where they are not likely to be able to be compromised.

It is important that non-sensitive information, such as name, address, phone number, or marketing data that may reflect the interests or shopping experiences of the individual, not be subject to notification. Such data is not likely to result in identity theft, and breach notification requirements tied to such data could result in unnecessarily alarming individuals.

3. National Data Security Standards Should Allow Flexibility for Businesses

The Task Force indicates that it is considering recommending national data security requirements for all commercial entities that maintain sensitive customer information, and requests comment on the "essential elements of such a requirement" and whether the need for such a standard "varies according to economic sector, business model, or business size."

The Commission's Gramm-Leach-Bliley Act ("GLB") safeguards serve as an appropriate framework for any entity possessing Social Security, driver's license, or financial account numbers. These standards should provide businesses with sufficient flexibility as to what is reasonable security based on the business model or business size. In addition, these standards should serve as a uniform national standard, so as to avoid multiple and potentially conflicting standards.

4. *Businesses are at the Forefront of Providing and Implementing Tools to Prevent Identity Theft*

Businesses are at the cutting edge of developing and implementing many of the technologies and procedures that can help combat identity theft. In order to be effective, many of the best tools ironically require that businesses have more, not less, ability to use personal information. Thus, the Task Force should be very cautious in making any recommendations that could limit access to personal information, thereby making it more difficult for businesses to use tools to prevent identity theft that rely on such information.

DMA believes that the Task Force should emphasize the important role that the business community already plays in completing billions of transactions annually with no instance of identity theft. It is critical for continued success that the business community be recognized for its contributions to protecting consumers from fraud and identity theft, and its partnership with law enforcement officials in combating bad actors. A major result of the Task Force's efforts should be to strengthen the public's confidence in commerce, particularly electronic commerce. Any message that incorrectly paints the business community as part of the problem would undercut this goal.

5. *Increased Educational Efforts Should be an Essential Part of the Task Force Recommendations*

The Task Force asks whether it should recommend a public awareness campaign to better educate consumers on how to safeguard their personal data. DMA would strongly support such an initiative, just as it now supports the Commission's consumer education efforts. In our experience, the most effective means of combating misuse of personal data is a well-informed and empowered individual. We believe that the essential elements of such a campaign are already present in the *AvoID Theft* campaign that the FTC has developed, and that those efforts could be expanded through greater resources and expanded partnerships with business, community, and consumer groups.

Thank you for the opportunity to submit these comments. Please contact me with any questions.

Sincerely

Jerry Cerasale

Jerry Cerasale
Senior Vice President, Government Affairs

cc: Stuart Ingis, Venable LLP